中国密码学会 译介

中国工程院院士 沈昌祥、蔡吉人 推 介

中国密码学会理事长 裴定一 作 序

北京科普创作出版专项资金资助

密码的奥秘

THE SECRETS OF CODES

[美] 保罗·伦德（Paul Lunde）编著

刘建伟 王 琼 等译

中国工信出版集团

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

中国密码学会 译介

密码的奥秘

THE SECRETS OF CODES

[美]保罗·伦德(Paul Lunde) 编著

刘建伟 王 琼 等译

電子工業出版社
Publishing House of Electronics Industry
北京 · BEIJING

版权贸易合同登记号　图字：01-2014-3647

图书在版编目（CIP）数据

密码的奥秘 /（美）伦德（Lunde,P.）编著；刘建伟等译. — 北京：电子工业出版社，2015.3
书名原文：The secrets of codes: understanding the world of hidden messages

ISBN 978-7-121-25376-8

Ⅰ. ①密… Ⅱ. ①伦… ②刘… Ⅲ. ①密码－普及读物
Ⅳ. ① TN918.2-49
中国版本图书馆 CIP 数据核字（2014）第 313652 号

策划编辑：张　冉（zhangran@phei.com.cn）
责任编辑：张　冉
印　　刷：北京盛通印刷股份有限公司
装　　订：北京盛通印刷股份有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱
　　邮编：100036
开　　本：787×1092　1/12　印张：24　字数：446 千字
版　　次：2015 年 3 月第 1 版
印　　次：2015 年 3 月第 1 次印刷
定　　价：128.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

目录

欢迎关注新浪微博@智思者，或加入智思者联盟QQ群（群号372899584），参与编辑，读者之间的交流互动，更有机会获赠精品图书。

本书内容涉及多个学科和不同文化背景，编辑工作难免疏漏，诚挚欢迎读者来信批评指正！交流 / 书评 / 投稿 / 纠错请联系：张冉，邮件 zhangran@phei.com.cn，微信号 olivia740139。

版权贸易合同登记号　图字：01-2014-3647

图书在版编目（CIP）数据

密码的奥秘 /（美）伦德（Lunde,P.）编著；刘建伟等译. — 北京：电子工业出版社，2015.3
书名原文：The secrets of codes: understanding the world of hidden messages

ISBN 978-7-121-25376-8

Ⅰ. ①密… Ⅱ. ①伦… ②刘… Ⅲ. ①密码—普及读物
Ⅳ. ① TN918.2-49
中国版本图书馆 CIP 数据核字（2014）第 313652 号

策划编辑：张　冉（zhangran@phei.com.cn）
责任编辑：张　冉
印　　刷：北京盛通印刷股份有限公司
装　　订：北京盛通印刷股份有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱
　　邮编：100036
开　　本：787×1092　1/12　印张：24　字数：446 千字
版　　次：2015 年 3 月第 1 版
印　　次：2015 年 3 月第 1 次印刷
定　　价：128.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

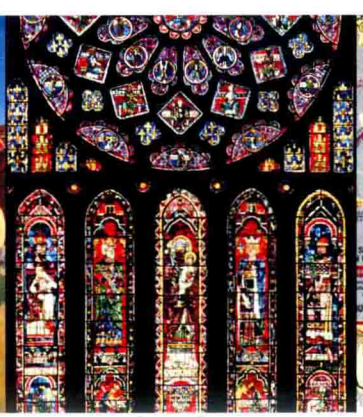
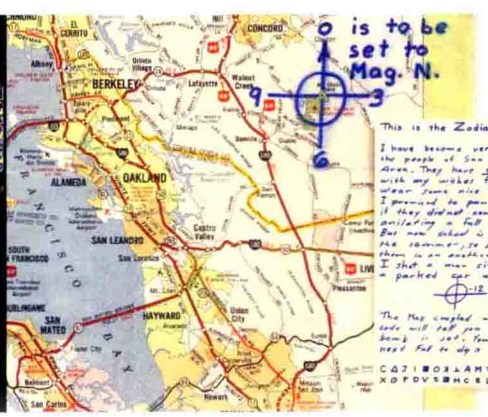
质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

目录

CONTENTS



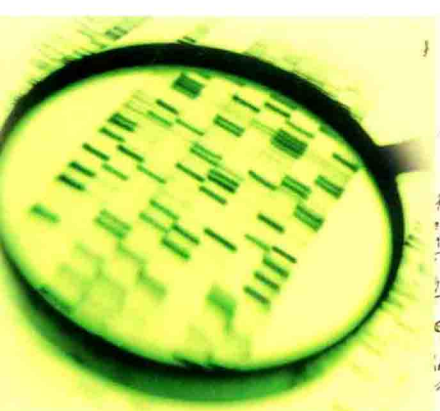
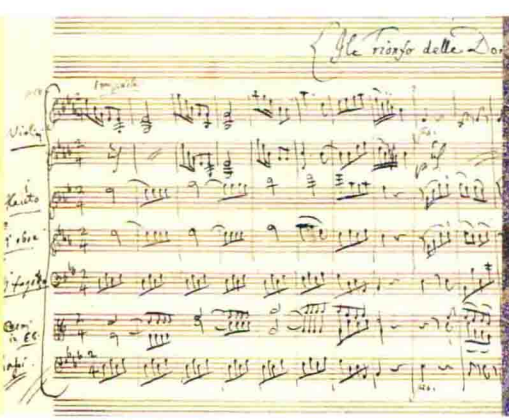
CONTENTS

06 黑社会暗号

07 编码世界

08 文明密码

09 商业编码

CONTENTS

10 人类行为代码

11 视觉符号

12 想象的密码

13 数字时代




中国密码学会 译介

中国工程院院士 沈昌祥、蔡吉人 推介

中国密码学会理事长 裴定一 作序

北京科普创作出版专项资金资助

密码的奥秘

THE SECRETS OF CODES

[美] 保罗·伦德（Paul Lunde）编著

刘建伟 王 琼 等译

中国工信出版集团

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

中国密码学会 译介

密码的奥秘

THE SECRETS OF CODES

[美] 保罗·伦德（Paul Lunde） 编著

刘建伟 王 琼 等译

電子工業出版社
Publishing House of Electronics Industry
北京 · BEIJING

序言

提到密码，很多人都会觉得它很神秘。本书是一本介绍密码知识的科普读物，它的目的是要帮助读者踏进密码知识的殿堂。它从介绍西方古代的加密方法开始，讲到两次世界大战中密码所发挥的神奇作用，最后介绍了当前信息化时代的现代密码的飞速发展。书中也讲述了不少与密码有关的故事。

本书较详细地介绍了古代西方智慧所提出的一些加密方法，这些方法往往并不复杂，例如恺撒密码，据文献记载，它是由罗马的恺撒大帝提出的。英文中有26个字母，它们依次排列为abcdefghijklmnopqrstuvwxyz。将明文中每个字母换成排在它后面第3位的字母，就得到密文。例如，codes的密文为frghv，收到信息的一方只要将密文中每个字母换成往前数3位的字母，就可还原得到明文。只要收方知道发方的加密方法即可。移动位数还可改为1~25中的任意一个数字，但发方与收方必须预先共同约定移动位数，这个位数称为密钥，它不能泄露给他人。如果希望加密方法更加复杂，可以要求不同位置的字母移动位置不是都一样的，这就是维吉尼亚密码。使用它时，需要选择一个密钥，决定每个位置字母的移动方法。维吉尼亚密码直到18世纪才被广泛使用。书中还介绍了几个中世纪被提出的影响较大的密码。现在看来，这些密码都不安全了。

传说从希腊时代开始，人们就在战争和外交中使用密码，罗马时代出现了上述的恺撒密码，可见战争对推动密码发展起了很大作用。

在第一次世界大战处于白热化的1917年，德国打算利用他们的潜艇对英法联军发起攻击。为了防止美国的介入，德国外交部部长给墨西哥总理发了一封加密电报，希望墨西哥向美国发动收复失地的战争，以牵制美国的军力，防止美国对德宣战。但这封加密电报被英国破译并告诉了美国，使得原先置身事外的美国提前对德宣战。

英国在第一次世界大战中破译了德国的密码。德国得知这一消息后，研制出更安全的恩格玛密码机，并应用于第二次世界大战。只要掌握了当天的密钥，用密码机输入明文就可输出密文，输入密文就可输出明文，非常便于使用。德军每天用它发送大量战场信息。英国和美国开足马力，研究其破译方法。最后，恩格玛密码被波兰的几位数学家成功破译。当时，年轻的数学家阿兰．图灵在英国的密码分析中心从事破译恩格玛密码的工作，他在波兰数学家的基础上取得了新进展，最终促成第一台编程计算机的诞生。

如今，密码的应用早已不再限于军事和外交，而

是扩展到金融和商业等领域。在传统的密码系统中，收方和发方都使用同一密钥加密或解密，如上文提到的恺撒密码和维吉尼亚密码；但在计算机网络通信广泛应用的环境中，要使发方和收方都预先约定所使用的密钥是很麻烦的。所以在20世纪70年代，提出了一种新型密码——公钥密码。在此类系统中，每个用户都有两个密钥——一个公钥和一个私钥，免除了预先约定密钥的烦恼。在公钥密码的研究中，应用了更多的数学方法。计算机的广泛应用，为密码的使用提供了强有力的工具。现在的密码算法都在计算机上通过编程软件实现，或者在芯片上通过电路硬件实现。

本书除了介绍密码知识之外，还介绍了生活中经常遇到的许多编码系统，如各种符号标志、乐谱、体育裁判的各种手势，等等，它们虽然不是严格意义上的密码，但也有传递信息的功能。本书图文并茂、深入浅出，编排风格灵活生动，能激发人们阅读的兴趣，是一本很好的密码知识科普读物，对于不同知识层面的读者，都值得一读。最后，还要感谢刘建伟和王琼等人为本书的翻译所付出的辛勤劳动。

裘宗一

2015年元旦



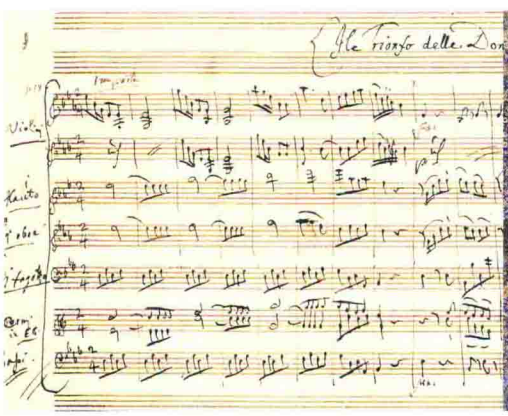

译者序

近年来，国内已经出版了很多用于高等教育的密码学教材，但真正能让非专业人士读懂的密码学科普读物非常鲜见。此外，市场上同样缺乏适合中学以上学生阅读的密码学科普图书。此书图文并茂，从古典密码学开始，引用古今中外大量有关密码编码学与密码分析学的实例，将深奥莫测、晦涩难懂的密码学原理，通过生动形象的语言及妙趣横生的图片娓娓道来，让读者在阅读故事的过程中了解密码学的演化和发展历史，体会密码学的无穷奥妙与魅力，引发读者对密码学的兴趣，点燃读者探究密码世界的热情。此书也有助于提高全社会的网络安全意识，相信它一定会得到广大读者的喜爱。

我们受中国密码学会的推荐和电子工业出版社的委托担任本书的译者。当我们第一次翻阅原版英文书时，便被此书的内容深深打动，感觉此书无疑是一本非常好的密码学科普读物。出于一种责任感，我们欣然接受了此书的翻译工作。然而，随着翻译工作的展开，这种兴奋的感觉荡然无存，甚至多次萌生放弃的念头。读者在阅读时也许会发现，此书涉及的学科跨度很大，涵盖历史、文化、宗教、艺术、生物、音乐、建筑、出版、体育、通信、计算机等多个学科，远远超出了我们的专业知识范围，翻译的难度可想而知。为了确保翻译质量，我们不仅要对原文进行反复推敲，有时还要查阅相关资料，翻译进度非常缓慢。与翻译普通英文书籍不同，此书的排版也极具挑战性，我们投入了大量的时间和精力以确保排版的准确性。如果没有我夫人王琼作为专业翻译所具有的耐心和坚持，我也许早就打了退堂鼓。因此，我由衷地佩服她所具备的出色翻译能力、坚强意志和专业素质。毫不讳言，没有她的倾尽全力和持之以恒，就没有此书的问世。

翻译工作追求“信、达、雅”。然而，说起来容易做起来难。例如，对原版书中有关“Code”一词的翻译，就斟酌再三。本书中的“Code”，原本是指人类发明的用来表示信息的代码。如果将书名翻译为“代码的奥秘”，则很容易让读者误认为此书为介绍计算机代码的书籍。在本书中，除了将“Code”翻译为“密码”之外，还根据它在不同章节中所代表的确切含义，分别译成“代码”、“编码”、“符号”、“暗号”等。需要说明的是，在翻译过程中，我们也发现原书中存在一些错误，例如，对中国文化理解有误、一些数据不准确，尤其是原理上的错误，如果不加以纠正，可能对读者造成误导。因此，译者在翻译时对原文进行了修正，并加以标注。

为使此书的翻译更加严谨，中国密码学会和电子



工业出版社特邀请了中国工程院院士蔡吉人、广州大学教授裴定一、密码科学技术国家重点实验室主任冯登国、西安电子科技大学教授王育民、北京邮电大学教授杨义先、中国密码学会秘书长于艳萍等专家在北京召开了一次审读会。他们对本书的翻译工作提出了很多很好的意见和建议。我的导师王育民教授专门写了一封长信，对本书的翻译提出了很多中肯的建议。我们也对书稿进行了反复修改，并已充分汲取了各位专家的意见和建议。在此，我们对各位专家的支持和帮助致以衷心的感谢。

此书的翻译出版得到中国密码学会和电子工业出版社的高度重视和大力支持。衷心感谢中国密码学会理事长裴定一和秘书长于艳萍的信任和举荐，并诚挚感谢沈昌祥院士、蔡吉人院士等诸位业内专家的精彩推荐。还要感谢中国密码学会的刘娟女士，她热情地承担了繁重的组织和协调工作，为此书的顺利出版做出了贡献。感谢此书的责任编辑张冉为此书付出了辛劳。她良好的沟通能力、出色的编辑水平及严谨而勤奋的工作态度，令我钦佩。

感谢参与本书翻译工作的我的博士研究生陈杰、王朝、何双羽、王蒙蒙、刘巍然、程东旭、周星光、刘哲，以及硕士研究生艾倩颖、吕盟、苏航、童丹、f夏丹枫、王志学、周云雅、陶芮、王培人等。感谢薛欢，她承担了索引的翻译和整理工作。感谢北航生物与医学工程学院的郑丽沙博士为此书翻译提供的帮助。

在翻译此书的日子里，我失去了挚爱的父母亲，经历了人生中最艰难和悲伤的一段时光。父母恩泽，重如泰山。谨以此书献给含辛茹苦养育我们的父母亲。

虽然我们已经竭尽全力确保翻译的质量，但由于时间仓促，并受译者知识面和翻译水平所限，翻译中的错误和不当之处在所难免，恳请广大读者提出宝贵意见和建议。

2015年元旦于北京航空航天大学




前言

我们都是熟练的“解读专家”。我们生活在一个由海量“代码”支撑的全球文化环境中，这个环境决定着我们的行为，它在向我们提供信息的同时，也将关于我们的信息传播出去。

早在咿呀学语之前，孩童们就已经开始解读自己周围的环境了，他们本能地观察和理解他人的表情和手势，从一开始就对声音十分敏感。要知道，语言理解是极其复杂的解码过程，除了要掌握大量语音外，还需要精通组合这些语音的规则，以及了解其他能传递额外信息的各种因素，如手势、声调和面部表情等。终其一生，人人都在下意识地不断解码，对周遭环境进行评价和估算。我们甚至可以听出弦外之音，因为语言除了用来表达，还能用于隐藏，例如在没有说出口的话里，其实也可以包含着信息。

“code”（本书译为“密码”、“编码”或“代码”等）一词，既表示一个有规则或法则的系统，也表示通信中所隐蔽的信息——这种语义上的多义性其实并不少见。英文中“dress code（着装规范）”和“code of behavior（行为准则）”中的“code”是指一系列规则，但若要让这些规则生效，还必须经由观察者来解读。“加密”对每个人都很重要，从“行为辨识”出现至今，“加密”可能都同等重要。一个人的穿着打扮和举手投足，都能够传递明确的信息。在现实社会中，这些信息可以十分复杂，暗含着包括年龄、性别、宗教、出身、地位等很多信息，甚至能够全面描绘某人的特征。

我们还必须解读周围的物理环境。早期人类曾通过解读所处的外部世界来辨识食物、发现危险，而人类正是依赖于这种能力才生存下来。这些能力涉及识别符号、解读地形和天气、提高跟踪技能、根据天体的运动来判断时间，以及了解季节更替的规律，等等。在现代城市中，人们也许已经忽略了上述技能，但如果想要生存下去，仍然需要具备足够的“信息解密”能力来正确地解读诸如广告栏、紧急出口和公路路标等。

“隐藏”似乎同样是人类常用的一种手段，许多组织都以特有的暗语和手势作为标志，或者用它来对外人隐藏消息。孩子们经常使用暗语来隐藏不想让大人们知道的事情，而成人也会巧妙而婉转地回避孩子们的好奇追问。在历史长河中，无论是盗窃团伙，还是统治精英，都曾用暗号或冷僻语种来向大众隐藏其真实想法。在某些社会群体中，即使语种相同，男女也会采用不同的表达形式。

作为语音的图形化表现，各种文字的发明能将之前许多转瞬即逝的东西持久地记录下来。文字本身就是某种编码，而针对一些古老失传的文字（如埃及象形文字或线性文字B）的“解密”，则只有在引入密码分析技术后才变得可行。作为一种精心隐藏信息的系统，“密码”也许与文字一样悠久。当然，文字为密码的出现提供了条件。

与现代国家一样，早期的原始部落也经常希望通过文字来隐藏信息（同时还能进行远程通信）。考古发现，远古时代就出现了军用加密技术，比如，令人眼花缭乱的各种“秘文”的使用，就贯穿了整个中世纪。

“加密系统”将原始消息中的词或短语置换成另一些字符，以此来隐藏原始消息中的秘密。早在16世纪，这种系统性的隐藏手段就开始在欧洲广泛应用。而每一种新的加密方式都会引出新的解密技术，这种“魔高一尺，道高一丈”的较量，曾在第二次世界大战中破解德国的恩格玛密码的传奇故事中达到了顶峰。通信技术的变革给密码编码者带来了新机遇，同时也为密码破译者提出了全新挑战。

今天，随着计算机通信系统的发展，密码已经从军用领域走进我们的日常生活。我们拨通的每个电话、发出的每封邮件都可以被自动“加密”，而实现这种奇迹的是相应的各种加密系统、设备和算法。同样，所有密文都可能被截获并破解。正如比尔·盖茨描述的那样，当今时代，最有价值的商品是“密码”以及由其分析获得的“内在”信息。为保护这些信息，加密系统必须不断升级，但正如每种编码都有相应的解码方案一样，任何一个加密系统最终都会被破译。这已经不仅仅是专家们需要考虑的问题了！在电子时代，最炙手可热的问题之一是如何保护人们的隐私，同时还要保护社会免于隐私滥用。

书中涵盖了几乎所有类型的“密码”的使用方式，这些“密码”都曾被用来传递各种信息。本书将“密码”类型按照彼此的相关性划分成不同的组，然后具体呈现属于特定类型的各种具体的“密码”。尽管各个主题部分（即每两页一小节的内容）大体按照时间顺序排列，但不同部分间的相互参照可以更好地揭示出清晰的密码世界。我们的周围是一张用密语编织成的网，而了解这张网，对我们的生存和成功都具有前所未有的重要性，所以，这是一本可以改变你人生的书！

保罗·伦德（Paul Lunde）